## AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

Please cancel claims 2, 3, 4, 7, 8, 11, 12, and 13 without prejudice.

Listing of claims:

1. (Currently amended) A computer-implemented method for managing sensitive data in a point-of-sale terminal having a processor having an internal first RAM and ~~first memory element, a processor having~~ a register, a security circuit, a second RAM external to the processor, and a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source, comprising:

storing sensitive data in the first RAM ~~memory element~~, wherein the sensitive data includes a general encryption key;

upon loss of power from the first source, switching to power from the second source, copying the sensitive data from the first RAM ~~memory element~~ to the register, and erasing the sensitive data from the first RAM ~~memory element~~; and

upon detecting an attack on the terminal, erasing the sensitive data from the first RAM ~~memory element~~ and from the register;

upon reapplication of power from the first source, copying the sensitive data from the register to the first RAM;

generating encrypted data using the general encryption key; and

storing the encrypted data in the second RAM.

2-4. (Canceled)

5. (Currently amended) The method of claim 1 **[[4]]**, further comprising:

generating a random value;

storing the random value in the first RAM~~memory element~~;

encrypting the random value as a marker value using the general encryption key;

storing the marker value in the second RAM ~~memory element~~; and

upon application of power from the first source, generating a temporary marker value from the random value stored in the first RAM ~~memory element~~ and the general encryption key, wherein an attack is detected if the temporary marker value is not equal to the marker value in the second RAM ~~memory element~~.

6. (Original) The method of claim 1, wherein the sensitive data includes a general encryption key.

7-8. (Canceled)

9. (Currently amended) An apparatus for managing sensitive data in a point-of-sale terminal having a processor having an internal first RAM and ~~first memory element, a processor having~~ a register, a security circuit, a second RAM external to the processor, and a power supply circuit arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source, comprising:

means for storing sensitive data in the first RAM ~~memory element~~, wherein the sensitive data includes a general encryption key;

means, responsive to a loss of power from the first source, for switching to power from the second source, copying the sensitive data from the first RAM ~~memory element~~ to the register, and erasing the sensitive data from the first RAM ~~memory element~~; and

means for detecting an attack on the terminal; and

means for erasing the sensitive data from the first RAM ~~memory element~~ and from the register in response to an attack on the terminal;

means, responsive to reapplication of power from the first source, for copying the sensitive data from the register to the first RAM;

means for generating encrypted data using the general encryption key; and

means for storing the encrypted data in the second RAM.

10. (Currently amended) A circuit arrangement providing for erasure of sensitive data, comprising:

a first RAM~~memory element~~;

a register;

a security circuit configured to detect a security threat to the circuit arrangement and generate a first signal upon detection of a security threat;

a power supply coupled to the first RAM ~~memory element~~, the register, and the security circuit, the power supply arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source; and

a second RAM; and

a processor coupled to the first and second RAMs, wherein the first RAM is internal to the processor and the second RAM is external to the processor, the processor further coupled to the register, the security circuit and the power supply, the processor configured to store sensitive data in the first RAM when power is available from the first source, wherein the sensitive data includes a general encryption key, and upon application of power from the second power source copy the sensitive data from the first RAM to the register and erase the sensitive data from the first RAM, wherein the processor is further configured to copy the sensitive data from the register to the first RAM upon reapplication of power from the first source, and generate encrypted data using the general encryption key and store the encrypted data in the second RAM.

11-13 (Canceled)

14. (Currently amended) The circuit arrangement of claim 10 ~~13~~, wherein the processor is further configured to generate a random value and store the random value in the first RAM ~~memory element~~, encrypt the random value as a marker value using the general encryption key and store the marker value in the second RAM ~~memory element~~, and upon application of power from the first source, generate a temporary marker value from the random value stored in the first RAM ~~memory element~~ and the general encryption key, detect an attack if the temporary marker value is not equal to the marker value in the second RAM ~~memory element~~.

15. (New) A payment terminal, comprising:

a keypad;

a card reader;

a display;

a processor coupled to the keypad, card reader and display, the processor configured to process transaction payment information input via the keypad and card reader;

a first RAM internal to and coupled to the processor;

a register internal to and coupled to the processor;

a second RAM external to and coupled to the processor;

a power supply coupled to the processor, first and second RAMs, the register, and the security circuit, the power supply arranged to provide power from a first power source when power is available from the first source and from a second power source when power is unavailable from the first source; and

a security circuit coupled to the processor and to the power supply, the security circuit configured to detect a security threat to the power supply and generate a first signal in response to detection of a security threat;

wherein the processor is configured to store an encryption key in the first RAM while power is available from the first source, responsive to application of power from the second power source copy the sensitive data from the first RAM to the register and erase the sensitive data from the first RAM, responsive to the first signal erase the encryption key from the first RAM and from the register, and generate encrypted data using the encryption key and store the encrypted data in the second RAM.

16. (New) The terminal of claim 15, wherein the processor is further configured to generate a random value and store the random value in the first RAM, encrypt the random value as a marker value using the general encryption key and store the marker value in the second RAM, and upon application of power from the first source, generate a temporary marker value from the random value stored in the first RAM and the general encryption key, detect an attack if the temporary marker value is not equal to the marker value in the second RAM.

17. (New) The terminal of claim 15, wherein the processor is further configured to copy the sensitive data from the register to the first RAM responsive to reapplication of power from the first source.